

WHAT IS CLAIMED IS:

1. A method of electronically signing documents,
comprising the steps of generating a token of delegation
from a first signatory to a second signatory, and
5 associating the delegation token with a document signed
electronically by means of a cryptographic key of the
second signatory, wherein the delegation token contains
delegation data electronically signed for the first
signatory, wherein the delegation data include an
10 identifier of the second signatory, and wherein the
delegation token is generated by a server in response to
a request sent by the second signatory in connection with
the signing of the document.
2. A method according to claim 1, wherein the electronic
15 signature performed by means of the cryptographic key of
the second signatory is applied to the document
accompanied by the delegation token.
3. A method according to claim 1, wherein the electronic
signature performed by means of the cryptographic key of
20 the second signatory is applied on the one hand to the
document and on the other hand to authenticated
attributes including the delegation token.
4. A method according to claim 1, wherein the delegation
token is associated with the document signed by means of
25 the cryptographic key of the second signatory without
itself being signed by means of the cryptographic key of
the second signatory.
5. A method according to claim 1, wherein the delegation
data further include data describing a validity period of
30 the delegation token.
6. A method according to claim 1, wherein the delegation

data further include description data of delegated powers conferred by the token.

5 7. A method according to claim 1, wherein the delegation token further comprises timestamp information for the token.

8. A method according to claim 1, wherein a revocation server is provided for storing information on possible revocation of the delegation token by the first signatory.

10 9. A method according to claim 8, wherein the delegation data further include an access address to the revocation server.

15 10. A method according to claim 1, wherein the delegation data are signed electronically by means of a cryptographic key of the first signatory.

11. A method according to claim 1, wherein the delegation data further include an identifier of the first signatory and are signed electronically by means of a cryptographic key of a third party.

20 12. A method according to claim 1, wherein the delegation token is associated by the second signatory with the document signed electronically by means of a cryptographic key of the second signatory.

25 13. A method according to claim 1, wherein the delegation token is sent to the second signatory by the server.

14. A method according to claim 13, wherein the delegation token is associated with the signed document by an applet downloaded from the server to a station of the secondary signatory.

15. A method according to claim 1, wherein the second signatory signs the document electronically and submits the signed document to the server, and wherein the server associates the signed document with the delegation token.
- 5 16. A method according to claim 1, wherein said request is accompanied by data depending on the document to be signed which are included in said delegation data to generate the delegation token.
- 10 17. A method according to claim 16, wherein said data depending on the document to be signed comprise a code obtained by hashing the document.
- 15 18. A computer device for electronic signature of documents by a second signatory delegated by a first signatory, comprising means for electronically signing a document by means of a cryptographic key of the second signatory, means for obtaining a token of delegation from the first signatory to the second signatory, and means for associating the delegation token with the signed document, wherein the delegation token comprises
- 20 delegation data electronically signed for the first signatory, wherein the delegation data include an identifier of the second signatory, and wherein the means for obtaining the delegation token are adapted to send a request relating to the signing of the document to a
- 25 server and to receive the token in response to said request.
19. A device according to claim 18, wherein the signature means are adapted to sign electronically the document accompanied by the delegation token, by means of the
- 30 cryptographic key of the second signatory.
20. A device according to claim 18, wherein the signature means are adapted to sign electronically on the one hand

the document and on the other hand authenticated attributes including the delegation token, by means of the cryptographic key of the second signatory.

21. A device according to claim 18, wherein the
5 delegation data further include data describing a validity period of the delegation token.

22. A device according to claim 18, wherein the delegation data further include data describing delegated powers conferred by the token.

10 23. A device according to claim 18, wherein the delegation data further include an access address to a revocation server storing information on possible revocation of the delegation token by the first signatory.

15 24. A device according to claim 18, wherein the delegation token further comprises timestamp information for the token.

25 25. A device according to claim 18, wherein said request is accompanied by data depending on the document to be
20 signed.

26. A delegation server for use in the electronic signing of documents by a second signatory delegated by a first signatory, comprising means for generating a token of delegation from the first signatory to the second
25 signatory in response to a request sent by the second signatory in connection with the signing of a document, wherein the delegation token contains delegation data electronically signed for the first signatory, and wherein the delegation data include an identifier of the
30 second signatory.

27. A server according to claim 26, further comprising means for sending the delegation token to the second signatory for association with the document signed electronically by means of a cryptographic key of the second signatory.

28. A server according to claim 27, further comprising means for uploading an applet to a station of the secondary signatory in order to control the association of the delegation token with the electronically signed document.

29. A server according to claim 26, wherein said request is accompanied by data depending on the document to be signed which are included in said delegation data to generate the delegation token.

30. A server according to claim 26, wherein said data depending on the document to be signed comprise a code obtained by hashing the document.

31. A server according to claim 26, further comprising means for receiving the signed document from the second signatory, and means for associating the signed document with the delegation token.

32. A server according to claim 26, wherein the delegation data further include data describing a validity period of the delegation token.

33. A server according to claim 26, wherein the delegation data further include description data of delegated powers conferred by the token.

34. A server according to claim 26, wherein the delegation token further comprises timestamp information for the token.

35. A server according to claim 26, wherein the delegation data further include an access address to a revocation server provided for storing information on possible revocation of the delegation token by the first signatory.

36. A server according to claim 26, wherein the delegation data further include an identifier of the first signatory and are signed electronically by means of a cryptographic key of a third party.

37. A computer program product to be installed in a computer device for electronic signature of documents by a second signatory delegated by a first signatory, comprising instructions for carrying out the following steps when the program is run by processing means of said device:

- sending a request to a delegation server in connection with the signing of a document;
- receiving a token of delegation from a first signatory to a second signatory, generated by the server in response to said request, wherein the delegation token contains delegation data electronically signed for the first signatory, wherein the delegation data include an identifier of the second signatory;
- electronically signing the document by means of a cryptographic key of the second signatory; and
- associating the delegation token with the signed document.

38. A computer program product according to claim 37, wherein the electronic signature performed by means of the cryptographic key of the second signatory is applied to the document accompanied by the delegation token.

39. A computer program product according to claim 37,
wherein the electronic signature performed by means of
the cryptographic key of the second signatory is applied
on the one hand to the document and on the other hand to
5 authenticated attributes including the delegation token.

40. A computer program product according to claim 37,
wherein the delegation token is associated with the
document signed by means of the cryptographic key of the
second signatory without itself being signed by means of
10 the cryptographic key of the second signatory.

41. A computer program product according to claim 37,
including an applet downloaded from the server to said
computer device.

42. A computer program product according to claim 37,
15 wherein said request is accompanied by data depending on
the document to be signed which are included in said
delegation data to generate the delegation token.

43. A computer program product according to claim 42,
wherein said data depending on the document to be signed
20 comprise a code obtained by hashing the document.

44. A computer program product to be installed in a
delegation server involved in the electronic signature of
documents by a second signatory delegated by a first
signatory, comprising instructions for carrying out the
25 following steps when the program is run by processing
means of said server:

- receiving a request from the second signatory in
connection with the signing of a document; and
- generating a token of delegation from a first
30 signatory to a second signatory in response to said
request, to be associated with the document signed

electronically by means of a cryptographic key of the second signatory,

wherein the delegation token contains delegation data electronically signed for the first signatory, wherein
5 the delegation data include an identifier of the second signatory.

45. A computer program product according to claim 44, further instructions means for sending the delegation token to the second signatory for association with the
10 document signed electronically by means of the cryptographic key of the second signatory.

46. A computer program product according to claim 45, further comprising instructions for uploading an applet to a station of the secondary signatory in order to
15 control the association of the delegation token with the electronically signed document.

47. A computer program product according to claim 44, wherein said request is accompanied by data depending on the document to be signed which are included in said
20 delegation data to generate the delegation token.

48. A computer program product according to claim 44, wherein said data depending on the document to be signed comprise a code obtained by hashing the document.

49. A computer program product according to claim 44,
25 further comprising instructions for receiving the signed document from the second signatory, and instructions for associating the signed document with the delegation token.

50. A computer program product according to claim 44,
30 wherein the delegation data further include data

describing a validity period of the delegation token.

51. A computer program product according to claim 44, wherein the delegation data further include description data of delegated powers conferred by the token.

5 52. A computer program product according to claim 44, wherein the delegation token further comprises timestamp information for the token.

53. A computer program product according to claim 44, wherein the delegation data further include an access
10 address to a revocation server provided for storing information on possible revocation of the delegation token by the first signatory.

54. A computer program product according to claim 44, wherein the delegation data further include an identifier
15 of the first signatory and are signed electronically by means of a cryptographic key of a third party.